TESTIMONY OF

KERRY WEEMS

ACTING ASSISTANT SECRETARY FOR

BUDGET, TECHNOLOGY AND FINANCE

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

MARCH 16, 2004

Thank you for inviting me here before you today. It is an honor to have the opportunity to work with the subcommittee as it leads the effort to increase the security posture of all departments and agencies throughout the Federal Government. As the US Government's principal agency for protection of the health of all Americans, HHS is charged with carrying out a wide range of diverse missions that touch the lives of all Americans. Today, I would like to describe for you the extensive efforts undertaken to improve the security posture at HHS and to comply with federal legislative priorities.

The HHS mission covers a wide spectrum of activities including medical and social science research, prevention of infectious diseases, food and drug safety, financial assistance, child support enforcement, health, substance abuse treatment and prevention, comprehensive health services for Native Americans, the eradication of child abuse and care for the elderly. HHS consists of twelve Operating Divisions (OPDIVs), including eight agencies in the U.S. Public Health Service and three Human Services agencies that manage more than 300 programs with diverse missions. In addition, HHS is the largest grant-making agency in the Federal Government, providing approximately 60,000 grants per year.

In an effort to increase the efficiency with which HHS provides services to the public, HHS has greatly expanded its reliance upon information technology (IT). In its most recent Federal Information Security Management Act (FISMA) submission, HHS reported 222 systems, 13 programs and 77 contractor operations and facilities, all of which require IT security protection. HHS recognizes that a clearly defined and comprehensive IT security strategy is essential to continue supporting the delivery of critical health, safety, and wellness services to the public, and to safeguarding the information entrusted to HHS by the public.

I would first like to summarize the current state of information security within the Department, the actions underway to address identified weaknesses, and the

improvements that we are putting in place to improve our overall IT security management.

I am pleased to report that continual improvements are being made in the management of information security at HHS. We have thoroughly analyzed the previous findings of this subcommittee, as well as the audits and analyses of other groups such as the OMB and the Office of the Inspector General, and have used these as a foundation for our IT Security Program Plan and our Five Year IT Security Strategic Plan.

Similarly, we have built a solid foundation in policy and procedures for IT security operations and management, including a series of supporting guides to assist personnel throughout HHS in understanding and implementing security policies and OMB guidance. These policies and guides provide a common baseline standard for IT security throughout the Department, which OPDIVs can exceed if their business operations require stronger protections. We have published final versions of the following guides:

- Baseline Security Requirements Guide
- Configuration Management Guide
- Certification and Accreditation Guide
- Web Security Guide
- Risk Assessment Guide
- HIPAA Compliance Guide
- IT Penetration Testing Guide
- Incident Response Planning Guide

Updates were also made on previous policies to meet new guidance from OMB, specifically in the areas of Privacy Impact Assessments (PIAs), Plan of Actions and Milestones (POA&M), security performance measures and metrics, security program reviews, self-assessments, system characterization, and resource categorization. Additional updates were made to address newly emergent technologies, such as Voice-

Over Internet Protocol, wireless communications and wireless LANs, malicious code, system-to-system interconnection, peer-to-peer software and multifunctional wireless devices.

HHS has taken decisive steps to remediate the weaknesses identified in the last FISMA report. We have drafted new policy and issued guidance concerning the integration of security into system development life cycles. We have linked IT security with capital budgeting by improving our integration of IT security elements into our Exhibit 53 and 300 submissions, and we have augmented procedures for our IT Investment Review Board to ensure that IT security is addressed before new investments are made. We have implemented a streamlined, yet very intensive support structure that provides our OPDIVs with automated tools that improve and centralize data collection and reporting of FISMA POA&Ms and OMB management and reporting requirements through the HHS Information Security Data Management (ISDM) tool. HHS has also licensed an automated National Institute for Standards and Technology (NIST) 800-26 Self-Assessment tool, DataCure, Inc.'s Security Self-Assessment Tool (SSAT), to standardize and facilitate the Department-wide utilization of this important NIST guidance. These tools are supplemented by extensive coaching support, and monthly POA&M review meetings with the Information Security Officer of each OPDIV.

HHS has also drafted guidance addressing security certification and accreditation, and developed remediation plans for ensuring certification and accreditation (C&A) of all appropriate systems. C&A compliance has increased by 32% in the last six months and is well on its way to exceeding the goal of 90% C&A compliance by June 30, 2004. For systems that have not completed C&A, each system has a specific remediation plan targeting their path towards certification in order to enforce accountability for compliance with FISMA. Recently, security remediation plans have been expanded to track privacy impact assessments (PIA), as well as linkages between system security and capital planning relationships. The Chief Information Security Officer (CISO) has conducted reviews of the training and awareness policies and practices currently in

place for each OPDIV, developed gap analyses between these policies, established requirements and best practices, and issued guidance regarding the management of mandatory annual user security awareness training. Lastly, HHS is developing a Departmental Security Operations Center (SOC) that will significantly improve our incident response capabilities and institutionalize a more rigorous defense against malicious hackers and other threats.

Specifically, HHS has established a system of IT security-specific effectiveness and efficiency metrics that are used to track our progress throughout the year, rather than just through quarterly snapshots of status. Examples of these metrics include the percentage or number of systems with incident prevention, protection, and response capabilities, and the number of HHS employees who completed security awareness training, to name but a few. Metrics are updated and reviewed as required by departmental policy. These metrics enable IT security to be incorporated into the existing management information frameworks within each OPDIV, and will better illustrate the progress that an OPDIV has made in addressing security weaknesses and managing its IT security program. HHS is continuing to expand and refine these metrics to adapt to operational and regulatory changes and to provide ever-increasing usefulness for HHS management oversight.

In addition to this effort, HHS created and launched "Secure One HHS," a comprehensive program that blends targeted IT security technical support and assistance with managerial and operational changes designed to improve the methods and practices of all personnel with IT security responsibilities throughout the Department. This program provides the framework for adequately securing our information systems as required by the FISMA and is thoroughly described later in my remarks. In fulfilling this initiative, HHS continues to demonstrate its commitment to protect the health and welfare of the American public.

Drivers Towards Increased Security

A number of legislative, internal and external factors have guided HHS forward toward an enterprise wide approach to security. These factors include the following:

- **Emerging role of HHS as a key organization in the area of Homeland Security** – Certain Homeland Security initiatives, such as first-responder programs for biological, chemical, and terrorism attacks, and other domestic emergencies rely heavily on HHS resources and capabilities for information. Should key security functions be compromised during a crisis, critical information and IT resources could be compromised, worsening the impact of any emergency.

- **Growing Impact of Security** – As IT resources play an increasingly important part in fulfilling our mission of "improving the health, safety, and well being of the American people," our mandate requires us to protect those resources from the ever-increasing incidents of denial of service (DoS) attacks, computer viruses, system intrusions, and other malicious IT attacks.

- **Office of the Inspector General (OIG) Audits and Reports –** The HHS OIG conducts annual evaluations of the Department's information systems to identify weaknesses and determine vulnerabilities. These audits help substantiate that ongoing security protections meet both Federal guidelines and established IT security best practices, and enable HHS and OPDIV management to prioritize needed security improvements.

- **Secretary Priorities –** HHS Secretary Tommy Thompson has publicly stated that IT security is one of his top priorities. His One HHS vision also has ramifications within IT security: from the need to enhance communication and collaboration across HHS, to the need to consolidate IT infrastructures and common administrative systems while maintaining an overarching IT security program.

- **HHS Enterprise Strategic Goals**: IT security is directly integrated into three of HHS' five Enterprise Strategic Goals:
    - Provide a secure and trusted IT environment.
    - Enhance the ability of the Nation's healthcare system to effectively respond to bioterrorism and other public health challenges.
    - Achieve excellence in IT management practices.

- **HHS Enterprise IT Strategic Plan –** The HHS Enterprise IT Strategic Plan for FY 2003-FY 2008 defines the Department's IT mission, vision, goals, initiatives and measures including the development of an HHS IT security program.

Progress

In response to the above drivers, HHS has developed a comprehensive program to satisfy mission critical IT requirements. Three of the largest initiatives undertaken by the Department in FY2003 demonstrate the ongoing efforts to continuously strengthen the HHS security posture:

- **Critical Infrastructure Protection Plan and Project Matrix**
- **Creation and launch of the "Secure One HHS" program**
- **Increased implementation of Managed Security Services**

These initiatives reflect the Department's dedication to the rapid and sustained improvement of the IT security of the HHS information systems and the data that these systems transmit, process and store.

Critical Infrastructure Protection

The primary purpose of the CIP effort is to strengthen the Department's overall security posture in compliance with Homeland Security Presidential Directive/HSPD-7, which requires that the Executive Branch assess the cyber vulnerabilities of the nation's critical infrastructures – information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of federal, state, and local governments. This requirement is clarified in National Plan for Information Systems Protection Version 1.0

which states, "[t]he initial necessary step in preparing a defense of critical information systems and computer networks is a thorough assessment of the potential critical infrastructure system assets, interdependencies, and vulnerabilities."

The Project Matrix effort is an objective evaluation process designed to assist departments and agencies in determining their nationally critical functions and supporting infrastructure. While many of the Federal Government's infrastructure assets support national security, economic security, and public health and safety, not all require intensive protection activities. Project Matrix is designed to identify critical functions, services, and infrastructures that may require additional protections, so that resources are applied effectively and efficiently. HHS has been a leader in implementing Project Matrix.

The Critical Infrastructure Protection (CIP) initiative is centrally managed by Office of Information Resource Management (OIRM) and requires close coordination with all OPDIV Chief Information Security Officers (CISO) and Information Systems Security Officers (ISSO). CIP activities include revalidation of Project Matrix Phase I findings, Project Matrix Phase II analysis for CIP assets, Certification and Accreditation for CIP assets, FISMA corrective actions for CIP assets and update of the HHS CIP Plan and Automated Information Systems Security Program Handbook.

HHS launched its first Project Matrix effort in 1999, completing Phase I in 2000. Later legislation changed the Project Matrix methodology from an asset focused evaluation to one centered on function, thereby requiring HHS to revisit its Phase I work. In October 2003, HHS completed its revised Phase I, (the identification of critical functions and services and the primary supporting cyber and physical assets,) and successfully updated the CIP Plan. HHS depends on approximately 900 assets (both cyber and physical) to conduct day-to-day operations. The Department, with the assistance of the

Department of Homeland Security, identified twenty-four nationally critical assets and thirty critical functions.

The Department has initiated Project Matrix Phase II, the interdependency analyses on the critical assets. An interdependency analysis, or value chain analysis, is conducted on each nationally critical function and service in order to identify infrastructure functions, linkages, dependencies, potential vulnerabilities, and points of failure that could impact availability, reliability, and security of the asset, thereby hindering its performance. By way of illustration, Phase II Value Chain analyses were completed for the following functions at FDA:

- Approving the marketing of biologic products to include blood, vaccines, tissue, allergenics and therapeutics;
- Providing health warning information regarding post-market drugs and biologic products.

We anticipate completing the interdependency analysis for both cyber and physical assets in 2006.

The steps in the Project Matrix methodology serve as the cornerstone of effective CIP management and provide important data to further infrastructure identification processes where assets are analyzed, dependencies recognized, vulnerabilities realized, threats identified and mitigation taken to prevent security weaknesses. One of the benefits of this effort is that it has improved the communication between HHS physical and cyber security operations as well as expanded the understanding of how cyber and physical assets interact. The information collected as part of this process is reported to OMB, as required by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" (A-130); Government Performance and Results Act (GPRA) Agency reports, and FISMA. Results of the analysis also provide information helpful to fulfilling reporting requirements, audits, risk mitigation and ensure efficient use of resources for security planning and budgeting.

Secure One HHS

Following Secretary Thompson's One HHS vision, we are implementing "Secure One HHS." The mission of Secure One HHS is to create an enterprise-wide secure and trusted IT environment in support of the overall HHS mission. Secure One HHS also identified program goals that define outcomes that support and enable the achievement of the Secure One mission. The Secure One HHS goals are the following:

Goal 1 **-** Improve the overall HHS IT security posture to protect confidentiality, integrity, and availability of IT resources.
Goal 2 **-** Ensure minimum security standards enterprise-wide, consistent with Federal guidelines and best practices.
Goal 3 - Support integration of IT security into HHS lines of business.
Goal 4 - Promote an environment where all employees' actions reflect the importance of IT security.

These goals provide the basis for development of the IT security program's action plans. The action plans provide detailed information on how the HHS IT security objectives will be executed, and are based on a results-oriented management approach. To ensure program success, Secure One HHS and the HHS CISO continuously track the progress of each action plan through a series of performance indicators.

As part of Secure One HHS, the Department has implemented a strong governance structure that clearly defines roles, responsibilities, and security expertise at both the Headquarters (HQ) and OPDIV levels. At the enterprise level, the Department CIO leads all Departmental IT efforts. At the OPDIV level, each OPDIV has its own CIO and IT security officer who is responsible for the IT security program within that OPDIV and responsible for compliance with the Secure One HHS Program.

This structure was selected because a "one size fits all approach" does not work for managing IT security within large and complex organizations like HHS. By managing

the program at the HQ level, HHS is establishing a consistent IT security foundation across the OPDIVs. However, by having OPDIVs control the implementation of HHS IT security policies, each OPDIV is empowered to incorporate or exceed standard HHS security controls consistent with their own unique operational risk levels and operating environments. For example, the HHS network connection security policy does not limit connections only to those from government owned equipment, whereas the FDA policy permits only FDA-owned equipment to connect to its internal network through its remote access solution. This policy helps FDA to ensure devices connecting to the FDA network are properly configured, and continuously maintained, and to adhere to the FDA security standards, thereby reducing the potential risk posed by poorly configured machines. This approach allows for the development of needed IT security standards while allowing the OPDIVs the flexibility and customization necessary to effectively protect their own systems, environments, and organizational missions.

Structurally, Secure One HHS is comprised of two distinct components: Program Development and Program Implementation. The Program Development component focuses on ensuring compliance with federal IT security mandates and regulations, as well as internal HHS goals and objectives (e.g., full certification and accreditation of Departmental systems). Additionally, the Program Development component determines the strategic direction of Secure One HHS. There are six focus areas supporting the Program Development component: Strategic Planning, Oversight and Evaluation (O&E), Performance Management, Policy and Guidance (P&G), Security Operations Center (SOC), and Security Architecture. The Program Implementation component provides targeted IT security implementation assistance to the OPDIVs. This implementation support helps enable the OPDIVs to achieve a consistent IT security baseline across the Department, while still allowing them to implement IT security measures commensurate with their own risk. Six focus areas compose the Program Implementation function: Service Design and Delivery (SD&D), Enterprise Integration (EI), Education and Awareness (E&A), Outreach, Privacy, and HHS Net.

Program Function	Description
Strategic Planning	*Develops the strategy of the maturing Secure One HHS and ensures that the strategy aligns with IT security priorities.*
Enterprise Integration	*Provides support and facilitates integration of IT security into enterprise initiatives.*
Policy and Guidance	*Coordinates and drafts policies and guidance in support of the maturing Secure One HHS.*
Oversight and Evaluation	*Reviews and evaluates Secure One HHS compliance with Federal Regulations, policy, and guidance.*
Education and Awareness	*Provides the data collection, analytical, instructional, and communications services required to assess current training initiatives, make recommendations, and produces and implements IT Security Education and Awareness products.*
Outreach	*Provides OPDIVs advisory services and implementation support, including FISMA surge support, and POA&M workshops, as part of a maturing Secure One HHS.*
Service Design and Delivery	*Develops and implements communications and service strategies to increase awareness, drive adoption, and build pride and trust in the Secure One HHS.*
Performance Management	*Provides process and technical infrastructure for quantifying all aspects of performance of the Secure One HHS, determining causes of problems, and empowering performance improvement within the context of mission priorities.*
Security Operations Center	*Provides the CISO with oversight and analytical capabilities as they relate to IT security incidents within the Department. Establishes incident reporting capability and ensures coordination of incident response with the OPDIVs. Also centralizes patch management services.*
Security Architecture	*Supports HHS EA vision by establishing enterprise-wide security standards and integrating security in the HHS lines of business and determines the requirements and standards for the target architecture.*
Privacy	*Develops and formalizes appropriate OCIO standards and management processes, resulting in the annual report of privacy compliance as required under Section 208 of the E-Government Act of 2002. This function is also responsible for collecting and monitoring privacy impact assessments at the department level.*
HHSnet Security Support	*Supports HHSnet development team to ensure appropriate IT security measures and safeguards are incorporated into the network infrastructure, thus increasing the IT security baseline across the Department.*

Key focus areas of the Secure One HHS Program currently include critical infrastructure protection (CIP), system and program level security development, and FISMA compliance, which includes numerous subcomponents such as C&A and incorporation of Plans of Action and Milestones (POA&M) as a management tool. Secure One HHS

enhances collaboration, communication and knowledge sharing within HHS and across the Federal Government. At the same time the enhancement for security to HHS assets provides safety and service to the American public through increased access to data and information.

The specific focus areas and activities of Secure One HHS have been developed to address the range of security practices and needs required by the diverse HHS enterprise and to support all IT security requirements. The focus areas give Secure One HHS the flexibility necessary to continue with its planned evolution. By targeting resources at specific IT security areas of focus, Secure One HHS is poised to continue to adapt to the changing nature of IT security threats and federal IT security requirements.

Ultimately, Secure One HHS contributes to the Department's maturing management programs and processes to improve the selection and evaluation of IT investments. HHS recognizes that all system security activities rely on an accurate and documented count of systems to ensure that sensitive information is protected. As such, establishing a comprehensive systems inventory has been a high priority in the Department. Our inventory efforts are closely interconnected with the HHS enterprise architecture efforts and remediation plans that are underway in order to benefit from synergies and consistencies across the enterprise.

At HHS, the relationship between the processes for IT system development and system inventory management and that of IT budgeting continues to expand. Justification of additional funds for existing projects as well as requests for new funding must account for security. One of the Secure One HHS standards is that all investments must be reviewed and approved by the CISO prior to submission to the IT Investment Review Board (ITIRB). If the project does not meet expectations in the area of security, the investment will not be allowed to proceed. Additionally, the ITIRB will not approve funding for projects without responsible risk management. HHS has also implemented a new capital planning and investment control (CPIC) policy and set of procedures to

reduce the risk of inadequate security protections as well as removing redundancies across investments enterprise-wide. We are also implementing a portfolio management tool that will enhance our visibility over IT investment projects and support the CPIC analysis. We believe the processes we have in place make capital planning and implementation at the program/system level more efficient, effective, and secure.

Managed Security Services

Managed Security Services includes 24/7 monitored Intrusion Detection Systems (IDS), vulnerability scanning, forensic analysis and related services. The Managed Security Services initiative has three key activities:

1. Establishing an incident response program which helps prevent, detect and manage information security incidents for HHS;
2. Providing a standardized process for identifying network vulnerabilities; and
3. Implementing a standardized process for responding to information security incidents in a timely manner.

The Managed Security Services activity includes 24/7 intrusion detection. Vulnerability scanning, security architecture, the installation of security prevention devices, and network monitoring services are other aspects of this Secure One HHS initiative. Over the past year, HHS has installed over three hundred additional intrusion detection devices and is in the process of installing another two hundred to provide an additional defense layer for the HHS network. The project also includes the addition of vulnerability scanning of HHS networks, servers and systems. The Managed Security Services initiative is a key component of the HHS Security Operations Center (SOC).

Integration of Security into Department wide initiatives

HHS is committed to ensuring enterprise wide security standards. Currently, three major Enterprise wide initiatives are underway, (UFMS, HHSnet, and the Small OPDIV

Infrastructure Consolidation,) all of which will require coordination and integration of high priority safeguards.

UFMS

Launched by Secretary Thompson as part of the One HHS initiative, the Unified Financial Management System (UFMS) directly supports the President's Management Agenda (PMA) for financial management reform by consolidating and improving internal controls and financial reporting for the Department.

UFMS has two major components -- a part to support CMS called the Healthcare Integrated General ledger Accounting System (HIGLAS), and a part to support the rest of the Department. The goal of the UFMS program is to have an integrated Department-wide financial system that consistently produces relevant, reliable and timely financial information to support decision-making and cost-effective business operations at all levels throughout the Department. Benefits include:

- Reducing the resources and infrastructure needed to perform financial operations;
- Reducing the number of information flows between the administrative and core financial systems;
- Streamlining both internal and external financial reporting, and enable consolidated HHS financial reporting; and
- Taking advantage of advanced technical capabilities.

From system inception, the HHS's enterprise wide UFMS has planned and provisioned to secure the system and protect its data. UFMS serves as a flagship for the Department for its thoroughness in proactively addressing security at all levels. Management, operational, and technical controls are being implemented, thus providing a robust protection hierarchy.

The Healthcare Integrated General ledger Accounting System (HIGLAS) will give CMS enhanced oversight of Medicare contractor accounting systems and will provide high quality, timely data for decision-making and performance measurement. The new system, which uses commercial-off-the-shelf software that has been certified by the Joint Financial Management Improvement Program, is an application solution that will reduce internal control weaknesses through the assignment of strict roles and responsibilities of all its users.

HHSnet

The Department of Health and Human Services (HHS) Office of Information Resource Management (OIRM) has initiated a department-wide effort to modernize and consolidate the HHS networking and computing environment to a common IT infrastructure with common administrative systems shared by all OPDIVs and Staff Divisions (STAFFDIVs). Consistent with the Secretary's One HHS vision, the effort calls for the consolidation of HHS Wide Area Networks (WANs) and the consolidation of multiple service providers to a single service provider and a shared network backbone for the HHS enterprise network. The resulting system is referred to as HHSnet.

While HHSnet is intended to facilitate collaboration and efficiencies of service among the organizations of HHS, the consolidated solution also targets the three primary principles of security: confidentiality, integrity and availability. Based on controls planed for the final solution, HHSnet participants will benefit from a heightened security stance that will not only offer more security for inter-department communications, but will establish redundancies and sharing capabilities to dramatically increase the availability of services, assets and data. By standardizing the security stance of the new system, HHSnet will achieve a level of trust amongst HHS entities that is currently unparalleled.

There are three phases associated with the implementation of HHSNet. Phase I, expected to be completed this April, focuses on establishing a common HHS network backbone that allows HHS data traffic to pass securely between OPDIVs on the Government managed network instead of using the internet for connectivity. The goal of Phase I is to consolidate network vendors for each OPDIV under a single set of security parameters and providing a more manageable security environment. This effort will reduce the total number of Internet pipes going into HHS and help us to better secure these access points.

Phase II focuses on the traffic and services shared between OPDIVs. The goal of Phase II is to establish the infrastructure and security necessary to facilitate collaboration among the OPDIVs. This phase establishes what can be easily referred to as a "business partners" network, and institutes a common level of trust between the OPDIVs, standardizing the manner in which traffic is routed and filtered between both enterprise services and OPDIV specific communications. HHS and OPDIV stakeholders are still considering the final design for adoption, but it will incorporate centralized incident monitoring and response and redundancy for disaster recovery purposes.

Phase III focuses on consolidating connections to the Internet. The goal of Phase III is to use centralized access to external resources while facilitating a standard set of security controls for inbound and outbound traffic. The final design is still under consideration, but will include a common firewall and intrusion detection solution to control inbound and outbound traffic.

OPDIV Infrastructure Consolidation

Small OPDIV Infrastructure Consolidation:

Prior to the implementation the HHS consolidation programs, OPDIVs relied on multiple helpdesks, call centers and network vendors to provide IT infrastructure support. One major consolidation effort that is greatly improving reliability, availability

and confidentiality of HHS data is the consolidation of IT Infrastructure of the small OPDIVs (AoA, ACF, AHRQ, OS, SAMSHA, OIG and PSC). The IT Service Center (ITSC) provides IT infrastructure support for these OPDIVs. Through this consolidation, HHS has reduced the number of IT infrastructure support FTE from 144 to 53. One support contract replaced eight existing support contracts. This will streamline trouble handling and security incident response. Service hours have been expanded for all locations; including 24x7 network monitoring and call center services allowing HHS to respond to network issues quickly, even during non-duty hours. A single Call Center has been established to accept and manage all service requests, giving the ITSC a broad picture of the health and welfare of the network environment. Plans to consolidate servers and network devices are being developed and will be implemented in the next 18 months. Software and network standards will be implemented during the same period. Through these measures the ITSC will be positioned to provide better monitoring, and support to our customers.

Large OPDIV consolidations

AS previously stated, prior to the implementation the HHS consolidation programs, OPDIVs relied on multiple point of IT infrastructure within an OPDIV. To give a few examples of the success of this effort:

During FY2003 National Institutes of Health (NIH) has**:**

- Consolidated 14 existing email services into one centrally managed service.
- Consolidated 25 existing IT Help Desks into one centrally managed service.
- Consolidated 16 wireless networks into one, improving interoperability and security.
- Consolidated Security: Reduced four internet access points to two (necessary for fail-over).

Centers for Disease Control (CDC) has been working on the enterprise consolidation of 6 specific infrastructure services in FY 2003.

- Completed email server consolidation in November 2003.
- Reduced remote access servers from 6 to 2 in September 30, 2003.
- Consolidated 16 helpdesks to one centrally managed service.
- Consolidated hosting services from 30 to 1 by establishment of a Mid Tier Data Center (MTDC) and hot site facility The MTDC initial operation began in July 2003. Network connectivity between hot site and MTDC was operational by September 30, 2003. Ten mission critical applications are operational in the MTDC with real-time data replication to the hot site and 4 more planned within 6 months. 165 servers and 33 Tera Bytes of data are managed under the MTDC.

Centers for Medicare and Medicaid Services (CMS) completed its IT consolidation in 2002. Lockheed Martin, under the Consolidated IT Infrastructure contract (CITIC), assumed responsibility for the various components of the CMS IT infrastructure: consolidation into a single integrated help desk, desktop services, voice communications, mainframe, mid-tier, and network services, and hardware/software maintenance.

Food and Drug Administration (FDA) established the Office of IT Shared Services in October 2003. As a result an RFP for a single source performance-based contract for IT infrastructure support was published on January 28, 2004. FDA has completely transitioned to HHSnet and in fact leads the implementation and design teams in that effort. FDA also appointed an Enterprise Architect that is aggressively moving forward with the establishment of and FDA wide Architecture in accordance with the HHS EA programs.

As with the ITSC and the small OPDIVs these consolidations will pay security dividends through better reporting measures, decreases in response time during a security event and providing a secure, stable platform to host and transport HHS data.

HHS Enterprise Architecture

HHS is currently developing an approach to integrate security within the HHS Enterprise Architecture. This approach is being designed to employ OMB's Federal Enterprise Architecture reference models, security standards and secure processes advanced within government and industry. In response to these challenges, HHS will integrate security into the HHS Enterprise Architecture focusing on lines of business rather than using a system centric approach. The approach has been based on the guidance of OMB and NIST security guidance to develop a blueprint for a business driven enterprise security architecture solution leveraging the federal enterprise.

This program is necessary to ensure the protection of information and information systems categorized as National Critical Infrastructure, National Security Information, HHS Mission Critical, and all other sensitive assets. Protection of these assets is required in accordance with Homeland Security Presidential Directive-7 (HSPD-7), Public Law 100-235 (Computer Security Act of 1987), OMB Circular A-130, Federal Information Security Management Act (FISMA), federal regulations, and Executive Branch directions.

HHS Enterprise Email System (HHS-EES)

The consolidation of multiple HHS email systems into a single department wide e-mail system will improve the overall security of communications within the Department. Currently, there are over 200 e-mail servers, each with unique security, disaster recovery, and continuity of operations issues. By consolidating, the Department can ensure that all 75,000 users will have the same high standard of anti-virus protection, uniformly controlled physical and electronic system access, and improved system availability during emergencies. Additionally, by moving email systems out of potential terrorist targets, such as the NIH or CDC, the overall threat to the security of the system is reduced.

OPDIV SPECIFIC ACCOMPLISHMENTS

Centers for Disease Control

The Centers for Disease Control plays a critical role in protecting the public from the most widespread, deadly and mysterious threats against our health. CDC serves as the national focus for public health surveillance, bioterrorism preparedness, and outbreak investigations. Because of its importance for both Health and Human Services and Homeland Security, as well as the fact that it is a high profile target for malicious hackers and terrorists, the CDC has an especially significant need to protect its critical IT resources and the extremely sensitive and important information contained within them.

In the context of carrying out its mission, the CDC collects individually identifiable health information used to identify, monitor, and respond to disease, death, and disability among populations. This data must be protected to preserve individual privacy and respect individual dignity while maintaining the quality and integrity of health data.

CDC remains committed to federal and state public health information security and privacy practices, and is vigilantly implementing IT security controls to protect both the health and the privacy of the American public. During FY2003, CDC implemented a digital certificate program within the public health arena that enables for the secure and protected transmission of sensitive and critical information between public health organizations, including HHS. Over 6000 certificates were issued to external partners supporting 28 public health surveillance efforts. In addition, a special "two-factor authentication" program was established that allowed over 9,700 staff and partners to access the internal CDC network securely from virtually anywhere in the world.

CDC has also implemented the Secure One HSS intrusion detection initiative and installed both network-based and host-based intrusion sensors on critical systems and instituted full around the clock intrusion monitoring. This effort has enabled CDC to

increase the efficiency and effectiveness of its counter-intrusion activities. These technical and operational improvements have been complimented by an mandatory internal training program aimed at educating CDC employees and partners about the importance of IT security and their roles in protecting the information and IT resources with which the CDC has been entrusted. The CDC is proud to report that 99.92% of all employees have completed the security awareness training.

National Institutes of Health

The National Institutes of Health (NIH) is the principal biomedical research agency of the Federal government. NIH seeks to expand fundamental knowledge about the nature and behavior of living systems and apply that knowledge for improving human health and reducing the burdens resulting from disease and disability. The NIH also supports biomedical and behavioral research domestically and abroad, conducts research in its own laboratories and clinics, trains researchers and promotes the acquisition and dissemination of medical knowledge.

Researchers collaborating from around the world to solve complex health problems require a computing environment that balances the need for open scientific collaboration against protection of data falling into the wrong hands. In 2003, NIH changed its open network architecture to a restricted and consolidated firewall architecture that preserved the communications and collaborations necessary for NIH research and operations, but also dramatically reduced the potential for successful network intrusions. In addition, multiple virus walls, (including file stripping techniques,) were employed to enhance security in depth. These key network components have not only protected NIH against last year's worms and viruses but continue to provide protection against the latest round of attacks and attempted infections.

The NIH has coupled these technical improvements with changes in management and operations. The NIH CIO chairs a management committee that provides senior

leadership and direction on the NIH-wide IT security program. The committee evaluates issues related to the security and privacy of NIH IT systems and data, including but not limited to: (1) uniform and prioritized policy and procedures for system security problem avoidance and response; (2) appropriate technological approaches; (3) external access; and (4) backup and disaster prevention and recovery.

Operationally, the NIH Computer Security Awareness and Training Program is a highly successful initiative. More than 98% of NIH employees have taken the training, which applies an award-wining, web-based training approach. National and international organizations, including universities and medical schools, continue to request the course for their own staff. NIH provides a wide portfolio of IT security classroom courses that include basic security awareness to highly advanced training for IT security professionals. Timely and informative articles are included in agency newsletters (e.g., the importance of maintaining up-to-date patches and antivirus software), and brochures and extensive guidance documents are available to staff. Institute/Center IT security personnel pursue the HHS-sponsored professional certification courses, as well as advanced technical training to ensure knowledgeable, well-trained staff supports the agency. Additional training is offered at the monthly ISSO meetings, which are open to all IT security staff.

Food and Drug Administration

The Food and Drug Administration (FDA) ensures the safety of foods and cosmetics and the safety and efficacy of pharmaceuticals, biological products and medical devices.

Recently, the FDA successfully designed and implemented a remote access solution to enable authorized users to securely access internal FDA resources from non-FDA locations. Designed to allow only government (FDA) owned devices to remotely access its IT resources, the FDA secure remote access solution employs best-of-breed security technologies to provide "two-factor" user authentication and multiple layers of other protections to safeguard potentially sensitive data (such as pharmaceutical patent or

safety information) while it is resident on the computer and in transit. In an environment where innovative pharmaceuticals are reviewed to ensure that safe and effective products reach the market in a timely way, secure remote access is paramount to ensuring protection of both the integrity and sensitivity of this proprietary data.

In addition to its remote access solution, the FDA has implemented a robust security architecture, applying a "defense-in-depth" approach to ensuring adequate protection for its confidential information resources and its heavily visited public website. The implementation and continued enhancement of this security architecture, which includes various firewall technologies, an intrusion detection and monitoring capability, multi-layered virus protection and a security-focused extranet design, enables the FDA to more securely fulfill its mission.

The FDA has also successfully developed and implemented an information security awareness program to ensure that all users of FDA information systems receive adequate security training to perform their duties while meeting the IT security obligations. This training has focused on the user's responsibilities in maintaining operational continuity, reducing IT security risks, and meeting Departmental and Federal Government IT security rules and regulations.

FISMA Compliance Update

Since many of the gains mentioned above were realized after the FY 2003 FISMA cycle was complete, the 2003 FISMA evaluation does not fully reflect the current state of the IT security and privacy protections currently in place or in development throughout the Department.

In less than a year, HHS has made major progress employing an extensive security program and increasing the level of system security throughout HHS. The underlying cause for most of the weaknesses raised by the IG in the FISMA 2003 report stemmed

from the lack of an effective information security management program structure. Secure One HHS was created to respond to these weaknesses, and improvements are already being made. While there is more work to be done, significant progress has been made in the managerial, technological, and operational levels throughout the Department. HHS has made great strides in certification and accreditation, system inventory, integration of security into capital planning, development of policies and programs, training, and incident response. C&A compliance has increased by 32% in the last six months and is well on its way to exceeding the goal of 90% C&A compliance by June 30, 2004. For systems that have not completed C&A, each system has a specific remediation plan targeting their path towards certification in order to enforce accountability for compliance with FISMA. Recently, security remediation plans have been expanded to track privacy impact assessments (PIA), as well as linkages between system security and capital planning relationships.

Essential to managing the Department's security program is a comprehensive understanding of the number and severity of existing weaknesses. As such, Secure One HHS has created an automated POA&M reporting tool and has conducted POA&M monthly meetings, process reviews, and workshops for OPDIV personnel. Quarterly performance measures have also been implemented in order to improve the tracking of POA&M progress. As a result of these efforts, POA&Ms are also now used as a fully integrated IT management tool that tracks the correction of IT security weaknesses over time and effectively validates funding requests for IT security. The POA&M effort has been pivotal to improving management oversight by allowing comparison of multiple data sources to verify and validate the data received from OPDIVs.

Next Steps

Because the IT threat environment is ever changing and federal requirements must be adjusted to respond to these threats, HHS recognizes that our security program must continually adapt. The Department remains unwavering in its commitment to

continually seek out ways to improve the development, implementation, monitoring, and oversight of IT security. The evolving nature of IT at HHS demands that increased attention be placed upon IT security and its integration into the larger business and program culture of the Department and its OPDIVs.

HHS is streamlining its IT security data collection and tracking process, increasing management oversight and awareness, and reducing the overall time and resources expended for IT security reporting. When fully implemented this effort will result in more accurate, timely, and consistent data for budgetary and planning purposes. However, the existence of automated tools is not enough; they must also be intuitive to the user and provide a broad spectrum of actionable information. Therefore, HHS is transforming its current IT security data collection process into a true performance measurement initiative. Each Secure One HHS goal and objective has performance measures that not only allow for measurement of program implementation, but are also used to verify and validate the effectiveness and efficiency of implemented security measures, as well as their impact upon HHS mission and business lines.

One of the fundamental reasons for the establishment of Secure One HHS is to support the OPDIVs in adapting HHS IT security practices and incorporating them into their unique lines of business. The Secure One HHS Communications Plan is designed to facilitate this vision by developing a process to capture attention, gain understanding, and ensure cooperation as HHS expands and integrates its IT security measures.
In addition to the Secure One HHS Communications Plan, a stronger and broader IT security awareness program is being established to positively change and reinforce behavior consistent with HHS IT security policy. The IT security awareness training course, and IT security rules of behavior, focuses attention on computer and information security, creating sensitivity to threats and vulnerabilities, and reinforces the active application of recommended security practices. Together, the implementation of both the Secure One HHS Communications Plan and the IT Security

Awareness Plan provide the strategy for expanding stakeholder commitment to the IT security program and driving cultural change within the Department.

Conclusion

HHS has made significant progress in implementing a comprehensive IT security program. We recognize that a successful IT security strategy calls for the institutionalization of sound IT security practices that are essential for the safeguarding of the information entrusted to HHS by the citizens of this country. We remain committed to this goal as we continue to implement the Secure One HHS Program and HHS will continue to work to further improve and expand the capabilities of the HHS IT security program.

In closing, I would like to reemphasize that HHS has a long history of protecting information critical to the American public and is well aware of the critical importance of security. We continue to listen and learn, and, we continue to act to improve how we protect ourselves and preserve the public trust. We are doing our part to carry out Congress' will to safeguard our future – with confident commitment and determination.